February 22, 2012

NH Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Delaney:

Pursuant to New Hampshire's Right to Privacy Act, §359-C:1, we are writing to notify you of a data security event that involved our company, Accucom Corporation, located in Boston, Massachusetts. The security event affected 12 New Hampshire residents. We immediately reported the situation to local authorities and the U.S. Secret Service, and have been working with them in their on-going investigation. The details of the security event and steps we have taken to mitigate the situation, are below.

NATURE OF THE SECURITY EVENT

We recently learned that on January 3, 2012, someone outside of our company used our credentials to make an unauthorized $1.00 charge to a number of customer payment cards that had previously been used by customers to make an authorized purchase through one or more of our affiliated websites. The activity raised our suspicion and so we promptly commenced an investigation and notified the local authorities, as well as the U.S. Secret Service. We have since learned that the charge activity was initiated from an IP address likely located in Vietnam. It remains unclear how our credentials or the customer payment card numbers were obtained. However, as detailed below, we have taken steps to mitigate the situation, including sending notice of the unauthorized access to affected New Hampshire residents, and increasing security measures.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

The security event affected 12 New Hampshire residents. Simultaneously with this letter, we sent a notice via first class mail on February 22, 2012 (a template copy is enclosed) to the affected New Hampshire customers, encouraging them to take measures to help prevent and detect any misuse of their information (e.g. canceling their payment cards, monitoring statements, and how to place a fraud alert with the three major credit monitoring bureaus), and where to find information regarding identity theft prevention.

STEPS WE HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

We are taking appropriate steps to help prevent such incidents from occurring in the future. Upon learning of this incident, we immediately changed our credentials and made other adjustments to our security controls. We continue to work with the authorities to pursue the offender and we are continually evaluating and modifying our practices and the practices of our service providers, to enhance the security and privacy of all confidential and sensitive information entrusted to us.

Sincerely,

Alon Cohen
General Manager
Accucom Corp

Enclosures (1)

From: Accucom Corp.
745 Boylston St., Suite 202
Boston. MA, 02116

<<Date>>
Reference #<<ids>>

To: <<Name>>
<<Street Address>>
<<City, State Zip>>

Confidential/Privileged Communication

Dear <<Name>>:

We write to inform you of an incident of unauthorized access to your payment card number. You used a payment card to make an online purchase with our company, Accucom Corporation, through one or more of our affiliated websites, such as infopay.com. The authorized charges on your card would have shown up on your statement as being from "Accucom" or "Infopay". For the reasons explained in more detail below, we recommend that you immediately cancel this card and then carefully check the card's statements for unauthorized activity.

What Happened To My Information? We recently learned that on January 3, 2012, someone outside of our company used our credentials to make an unauthorized $1.00 charge to a number of payment cards, including yours. The activity raised our suspicion and so we promptly commenced an investigation and notified the local authorities, as well as the U.S. Secret Service. We have since learned that the charge activity was initiated from an IP address likely located in Vietnam. It remains unclear how our credentials or your credit card number were obtained. However, it is possible that in addition to your payment card number, the name and billing address you entered to make your authorized purchase on our website may also have been accessed without authorization. As a result, we are sending you this letter to inform you about what happened and suggest steps you can take to protect yourself.

What Should I Do Now? In some cases the $1.00 charge was immediately voided, so you may not see the $1.00 charge on your statement. However, we suggest that you promptly contact your payment card company to cancel the card and monitor your statement for any inappropriate activity.

What Other Steps Can I Take To Protect Myself? In addition to canceling your card and monitoring your statements, you also may wish to consider placing a fraud alert with the three major U.S. credit bureaus, Equifax, Experian, and TransUnion. To place a fraud alert on your credit report you can call any one of the bureaus listed below and they will contact the other two on your behalf.

An initial fraud alert remains on your report for a period of 90 days. You will receive a free credit report from each of the three companies and you should review the reports and your account statements carefully to identify any problems. A fraud alert on your credit report does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information may have been compromised and requires it to verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. While this may cause a short delay if you apply for the credit, the verification process protects you from having others applying for credit in your name.

Here is the contact information for the credit bureaus in case you have questions about the fraud alert or how to read your free credit report; you may also contact the credit reporting agencies to extend a fraud alert for a longer period of time or to reinstitute a fraud alert at a later date:

Equifax: 1 (800) 525-6285, www.equifax.com Fraud Division P.O Box 740250 Atlanta, GA 30374	**Experian**: 1-888-397-3742 www.experian.com P.O Box 1017 Allen, TX 75013	**TransUnion**: 1-800-680-7289, www.transunion.com Fraud Victim Assistance Division, P.O Box 6790 Fullerton, CA 92834-6790

We recommend that you closely monitor your financial accounts (particularly for the next 12-24 months) and, if you see any unauthorized activity, promptly contact your financial institution.

Because a victim's personal information is sometimes held for use or shared among a group of thieves at different times, checking your credit reports periodically can help you spot problems and address them quickly. You may want to consider requesting a free credit report. The federal Fair Credit Reporting Act ("FCRA") allows consumers to obtain a free copy of their credit report each year from the three major credit bureaus. The credit bureaus have established a centralized website, toll-free telephone number and mailing address for consumers to order their reports. Annual reports may be requested by:

1. Logging on to www.AnnualCreditReport.com
2. Calling: 1-877-322-8228
3. Writing: Annual Credit Report Request Service, P.O. Box 105281, Atlanta GA 30348-5281.

Please note that you will need to provide your full name, current address, social security number, date of birth and past addresses (if you have moved in the past two years), to obtain your free credit report.

The Federal Trade Commission (FTC) maintains a helpful website at www.consumer.gov/idtheft to help guard against identity theft and can be reached by telephone at 1-877-ID-THEFT (877-438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. The FTC recommends that you check your account statements and credit reports periodically. If you find suspicious activity on your credit reports or have reason to believe that your information is being misused, you should immediately call your local law enforcement office and file a police report. Make sure to get a copy of the report, as many creditors will want information contained in the report to absolve you of fraudulent debts.

You may also want to consider filing a complaint with your state's Attorney General and with the FTC. Your complaint will be added to the FTC's Identity Theft Clearinghouse, which law enforcement can access to aid in their investigations. Both your state Attorney General and the FTC can provide information about preventing identity theft.

For residents of Maryland, you can contact your Attorney General at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202 (1-888-743-0023) (www.oag.state.md.us).

For residents of North Carolina, you can contact your Attorney General at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699 (1-919-716-6400) (www.ncdoj.com).

What Else Do I Need to Know? We take the privacy and security of your information very seriously. We sincerely regret this incident occurred and we are taking appropriate steps to help prevent such incidents from occurring in the future. Upon learning of this incident, we immediately changed our credentials and made other adjustments to our

security controls. We continue to work with the authorities to pursue the offender and we are continually evaluating and modifying our practices and the practices of our service providers, to enhance the security and privacy of all confidential and sensitive information entrusted to us.

Should you have any questions regarding this letter or to confirm which payment card was involved in this incident, please call our customer service hotline at (800) 559-7449 or (617) 933-9946. If you receive a busy signal due to high call volume, please call back. If you are able to leave a voice mail, we will return your call promptly. If you prefer, you can contact Accucom at our mailing address: Accucom Corporation, 745 Boylston Street, Suite 202, Boston, MA 02116.

Thank you very much for your attention to this matter.

Sincerely,

Alon Cohen
General Manager
Accucom Corp